CIBSI 2009

16 al 18 de Noviembre
Montevideo, Uruguay

V Congreso Iberoamericano de Seguridad Informática

Actas del Congreso

Actas del V Congreso Iberoamericano de Seguridad Informática
CIBSI'09
Montevideo, Uruguay, 16 al 18 de Noviembre de 2009

Editores
Gustavo Betarte
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho

ISBN: 978-9974-0-0593-8

Prefacio

Estimados colegas:

Este volumen contiene los trabajos presentados en el V Congreso Iberoamericano de Seguridad Informática (CIBSI'09) realizado en Noviembre en Montevideo, Uruguay.

Esta edición del Congreso Iberoamericano de Seguridad Informática, iniciativa de la Red Temática Iberoamericana de Criptografía y Seguridad de la información CriptoRed, ha convocado al igual que en sus anteriores ediciones a un gran número de investigadores y expertos de Latinoamérica, España y Portugal.

De 65 trabajos recibidos, el Comité de Programa Científico ha seleccionado 41 trabajos, 38 de los cuales se presentan en el evento. Los mismos proceden de investigadores de Argentina, Brasil, Chile, Colombia, España, EE.UU., Francia, México, Portugal, Uruguay y Venezuela.

El congreso cuenta asimismo con tres conferencistas que han sido invitados a presentar su trabajo de investigación en sesiones plenarias, el Dr. Gilles Barthe, de IMDEA Software de España, el Dr. Eduardo Giménez, de la Universidad de la República de Uruguay y el Dr. José Luis Piñar Mañas de la Universidad CEU San Pablo de España. Tendrá también lugar en el congreso un taller, titulado *Los retos de la protección de datos: la Ley 18331 de protección de datos personales*, a cargo del Dr. José Luis Piñar Mañas.

Desde estas páginas queremos hacer llegar nuestro profundo agradecimiento a los organizadores, autores, revisores, patrocinadores y asistentes, que son los que han hecho posible que una vez más tenga lugar este encuentro académico de expertos e investigadores en Seguridad Informática, esta vez en la ciudad de Montevideo.

Noviembre 2009

Gustavo Betarte
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho
CIBSI'09

Organización de la Conferencia

CIBSI'09 es organizado por la Facultad de Ingeniería de la Universidad de la República en conjunto con la Universidad Politécnica de Madrid, a cuyos directivos asi como a todos y cada uno de los miembros del comité organizador queremos agradecer desde estas páginas.

Organización General

Gustavo Betarte, Universidad de la República, Uruguay
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España

Comité de Programa

Santiago Martín Acurio Del Pino, Pontificia Universidad Católica del Ecuador, Ecuador
Nicolás C.A. Antezana Abarca, Sociedad Peruana de Computación, Perú
Javier Areitio Bertolín, Universidad de Deusto, España
Walter Baluja García, Instituto Superior Politécnico José Antonio Echeverria, Cuba
Tomás Barros, NIC Labs, Chile
Gustavo Betarte (co-chair, Universidad de la República, Uruguay)
Joan Borrel Viader, Universidad Autónoma de Barcelona, España
Pino Caballero Gil, Universidad de La Laguna, España
Jeimy Cano Martínez, Universidad de los Andes, Colombia
Adriano Mauro Cansian, Universidade Estadual Paulista, Brasil
Hugo César Coyote Estrada, Instituto Politécnico Nacional, México
Enrique Daltabuit Godas, Universidad Nacional Autónoma de México, México
Jorge Dávila Muro, Universidad Politécnica de Madrid, España
Ángel Martín del Rey, Universidad de Salamanca, España
Josep Domingo-Ferrer, Universidad Rovira i Virgili, España
Josep Lluis Ferrer-Gomilla, Universidad de Las Islas Baleares, España
Amparo Fúster Sabater, Consejo Superior de Investigaciones Científicas CSIC, España
Luis Javier García Villalba, Universidad Complutense de Madrid, España
Roberto Gómez Cárdenas, ITESM Monterrey, México
Juan Pedro Hecht, Universidad de Buenos Aires, Argentina
Marco Aurelio Henriques, Universidade Estadual de Campinas, Brasil
Emilio Hernández, Universidad Simón Bolívar, Venezuela
Leobardo Hernández Audelo, Universidad Nacional Autónoma de México, México
Luis Hernández Encinas, Consejo Superior de Investigaciones Científicas CSIC, España
Alejandro Hevia, Universidad de Chile, Chile
Juan Guillermo Lalinde, Universidad EAFIT, Colombia
Javier López Muñoz, Universidad de Málaga, España
Julio César López, Universidade Estadual de Campinas, Brasil
Vincenzo Mendillo, Universidad Central de Venezuela, Venezuela
Carlos Mex Perera, ITESM Monterrey, México
Josep María Miret Biosca, Universidad de Lleida, España
Gaspar Modelo Howard, Universidad Tecnológica de Panamá, Panamá

Raúl Monge, Universidad Técnica Federico Santa María, Chile
Edmundo Monteiro, Universidad de Coimbra, Portugal
Guillermo Morales Luna, Centro de Investigación y Estudios Avanzados del IPN, México
Alberto Peinado Domínguez, Universidad de Málaga, España
Yoan Pinzón, Universidad Nacional de Colombia, Colombia
Tamara Rezk, INRIA Sophia Antipolis, Francia
Arturo Ribagorda Garnacho, (co-chair) Universidad Carlos III de Madrid, España
Josep Rifà Coma, Universidad Autónoma de Barcelona, España
Miguel Soriano Ibáñez, Universidad Politécnica de Cataluña, España
Horacio Tapia Recillas, Universidad Autónoma Metropolitana, México
Routo Terada, Universidade de São Paulo, Brasil
Alfredo Viola, Universidad de la República, Uruguay
Horst von Brand, Universidad Técnica Federico Santa María, Chile

Organización Local

Alejandro Blanco, Universidad de la República, Uruguay
Eduardo Carozo, ANTEL, Uruguay
Carlos Luna, Universidad de la República, Uruguay
Marcelo Rodríguez, Universidad de la República, Uruguay
Leonardo Vidal, Universidad de la República, Uruguay
Felipe Zipitría, Universidad de la República, Uruguay

Revisores Externos

Joao Afonso Abrunhosa, Universidade de Lisboa, Portugal
Almudena Alcaide, Universidad Carlos III de Madrid, España
Jorge Blasco Alis, Universidad Carlos III de Madrid, España
Philippe Camacho, Universidad de Chile, Chile
Eduardo Carozo, ANTEL, Uruguay
Eduardo Cota, Universidad de la República, Uruguay
Tiago Cruz, Universidade de Coimbra, Portugal
Eduardo Giménez, Universidad de la República, Uruguay
Jorge Granjal, Universidade de Coimbra, Portugal
Daniel Hedin, Chalmers University of Technology, Suecia
Julio César Hernandez-Castro, University of Southampton, Inglaterra
Jesús Manjón, Universitat Rovira i Virgili, España
Mireya Morales, Universidad Simón Bolivar, Venezuela
Gloria Pujol, Universitat Rovira i Virgili, España
Alejandro Russo, Chalmers University of Technology, Suecia
Miguel Torrealba, Universidad Simón Bolivar, Venezuela
Rolando Trujillo, Universitat Rovira i Virgili, España
Alexandre Viejo, Universitat Rovira i Virgili, España
Arnau Vives, Universitat Rovira i Virgili, España

Tabla de Contenidos

iPhone 3G: Un nuevo reto para la informática forense 1
Andrea Ariza, Juan Ruíz, Jeimy Cano

Uso del DNIe para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes 16
Emilia Pérez Belleboni, Justo Carracedo Gallardo

Command dimension reduction in masquerader detection 31
Carlos Benitez, Pablo Fierens

A Survey on Masquerader Detection Approaches 46
Maximiliano Bertacchini, Pablo Fierens

Propostas para apoiar a preservação documental de longo prazo na ICP-Brasil . . 61
Viviane Bertol, Rafael Timóteo de Sousa Júnior, Ricardo Custodio

Generación de ambientes para entrenamiento en seguridad informática 73
Alejandro Blanco, Juan Diego Campo, Lucía Escanellas, Carlos Pintado, Marcelo Rodríguez

Robust Declassification for Bytecode 88
Eduardo Bonelli, Francisco Bavera

Técnicas anti-forenses en informática: ingeniería reversa aplicada a TimeStomp . 103
Armando Botero, Ivan Camero, Jeimy Cano

Aplicar el modelo de amenazas para incluir la seguridad en el modelado de sistemas 118
Marta Castellaro, Susana Romaniz, Juan Carlos Ramos, Carlos Feck, Ivana Gaspoz

Sobre el número de funciones bent obtenidas a partir de funciones de máximo peso 133
Joan-Josep Climent, Francisco J. García, Verónica Requena

Um IDS Cooperativo para Redes de Acesso de Banda Larga 148
Tiago Cruz, Thiago Leite, Patricio Baptista, Rui Vilão, Paulo Simões, Fernando Bastos, Edmundo Monteiro

An Extended Reference Monitor for Security and Safety 163
Eduardo B. Fernandez, Michael VanHilst, David laRed Martinez, Sergio Mujica

Detección y limitaciones de ataques clásicos con Honeynets virtuales 173
Hugo Fernández, Jorge Sznek, Eduardo Grosclaude

Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos 188
Juan Pedro Hecht

Watermarking in the encrypted Domain 202
Jordi Herrera-Joancomartí, David Megías

La protección de datos y el diseño de tratamientos de datos personales. Especificaciones funcionales necesarias 213
Angel Igualada Menor

Una marca de agua inteligente aplicada al dinero electrónico 225
Patricia Jaimes, Gabriel Hermosillo, Gomez Roberto

Aumento de la fiabilidad de la evidencia en un protocolo de intercambio justo mediante la división del entorno de firma 240
Jorge L. Hernandez-Ardieta, Ana I. Gonzalez-Tablas, Benjamin Ramos Álvarez, Arturo Ribagorda Garnacho

Análisis formal del estándar NIST para modelos RBAC 255
Carlos Luna, Cristian Rosa

FACTOIDS: Modelos y Herramientas para el Análisis e Intercambio Seguro de Datos Colectados por Sensores 270
Carlos Martinez-Cagnazzo

Autorización de Acceso en MIDP 3.0 283
Gustavo Mazeikis, Carlos Luna

Diseño básico de la seguridad para un servicio sacional de salud pública en Venezuela 298
Mireya Morales, Emilio Hernández

Estegoanálisis aplicado a la generación automática de estegotextos en lengua española. 310
Alfonso Muñoz Muñoz, Justo Carracedo Gallardo

Metodología de implantación de un SGSI en grupos empresariales de relación jerárquica 325
Gustavo Pallas, María Eugenia Corti

Verificación formal de la equidad de un protocolo de firma de contratos mediante Colored Petri Nets 340
M. Magdalena Payeras-Capellà, Macia Mut-Puigserver, Andreu Pere Isern-Deyà, Josep L. Ferrer-Gomila, Llorenç Huguet-Rotger

Criptoanálisis del generador Auto-Shrinking: Una propuesta práctica 355
María Eugenia Pazo Robles, Amparo Fuster Sabater

Diseño e implementación de una función hash basada en caos 368
César José Ramírez López, Leobardo Hernández Audelo

Gestión Automatizada de Requisitos de seguridad para proyectos de desarrollo de líneas de producto Software 383
Jesus Rodriguez, Daniel Mellado, Eduardo Fernandez-Medina, Mario Piattini

SLSB: improving the steganographic algorithm LSB 398
Juan José Roque, Jesús María Minguet

Hacia una arquitectura de servicios de seguridad para entornos Grid móviles 409
David G. Rosado, Eduardo Fernandez-Medina, Javier Lopez

Gestión de identidad en las administraciones públicas: Interoperabilidad pan-Europea 423
Sergio Sánchez, Ana Gómez

MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES 437
Luis Enrique Sánchez Crespo, Daniel Villafranca Alberca, Eduardo Fernández-Medina Patón, Mario Gerardo Piattini Velthuis

Metodología para la selección de métricas en la construcción de un cuadro de mando integral 452
Daniel Villafranca Alberca, Luis Enrique Sánchez Crespo, Eduardo Fernández-Medina Patón, Mario Piattini

Towards Secure Distributed Computations 467
Felipe Zipitría

Protocolo de creación de evidencias en entornos vehiculares 482
José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, Benjamín Ramos

Control de calidad en imágenes de iris mediante razonamiento ontológico 497
Alberto de Santos Sierra, Javier Guerra Casanova, Carmen Sánchez Ávila, Vicente Jara Vera

Una propuesta de arquitectura biométrica de control de acceso basada en ontologías 509
Alberto de Santos Sierra, Javier Guerra Casanova, Carmen Sánchez Ávila, Vicente Jara Vera

Índice de Autores 520

MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES

Luís Enrique Sánchez[1], Daniel Villafranca[1], Eduardo Fernández-Medina[2] y Mario Piattini[2]

[1]SICAMAN Nuevas Tecnologías. Departamento de I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España.
{dvillafranca, lesanchez} @sicaman-nt.com
[2] Grupo de Investigación ALARCOS. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen. Con la creciente dependencia que la sociedad de la información tiene de las Tecnologías de la Información y las Comunicaciones (TIC), la necesidad de proteger la información tiene cada vez mayor importancia para las empresas. En este contexto, surgen los Sistemas de Gestión de la Seguridad de la Información (SGSI), que tienen una gran importancia para la estabilidad de los sistemas de información de las compañías. El hecho de poder disponer de estos sistemas ha llegado a ser cada vez más vital para la evolución de las PYMES. En este artículo mostramos la metodología desarrollada para el desarrollo, implantación y mantenimiento de un sistema de gestión de seguridad, adaptada a las necesidades y recursos de los que disponen las PYMES. Este enfoque está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

Palabras clave: SGSI, PYMES, Gestión de la Seguridad, Niveles de Madurez

1 Introducción

En un entorno empresarial globalizado y competitivo como el existente en la actualidad, las compañías dependen cada vez más de sus sistemas de información, pues se ha demostrado que tienen una enorme influencia para aumentar su nivel de competitividad. Pero sin una adecuada gestión de la seguridad estos sistemas de información carecen de valor real, ya que no pueden aportar las suficientes garantías de continuidad a las empresas. Por ello, las compañías empiezan a tener conciencia de la enorme importancia que tiene el poseer unos sistemas de seguridad de la información adecuados, así como una correcta gestión de los mismos. De esta forma, pese a que muchas empresas todavía asumen el riesgo de prescindir de las medidas de protección adecuadas, otras muchas han comprendido que los sistemas de información no son útiles sin los sistemas de gestión de seguridad y las medidas de protección asociados a ellos.

Gran parte de este cambio de mentalidad en las empresas tiene su origen en el cambio social producido por Internet y la rapidez en el intercambio de información, que ha dado lugar a que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos. De esta forma, las empresas ya han tomado conciencia de que la información y los procesos que apoyan los sistemas y las redes son sus activos más importantes [1]. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa. Así, la importancia de la seguridad en los sistemas de información viene avalada por numerosos trabajos [2, 3], por citar sólo algunos.

Anteriormente, las compañías que habían decidido proteger sus sistemas de información habían afrontado proyectos desde la perspectiva de que la seguridad era algo individual que afectaba a un objeto pero no al conjunto al que pertenecía el objeto, es decir, se basaban en la implantación de medidas de seguridad, pero sin llevar a cabo una adecuada gestión de dichas medidas [4]. Con el tiempo, al no disponer de una gestión adecuada, los controles implantados dejaban de mantenerse y se convertían en controles pasivos, que en lugar de ayudar a mejorar la seguridad contribuían a desinformar, ofreciendo información errónea en muchos casos. Así, en [5] se destaca que para la construcción de un sistema de seguridad no bastan los aspectos tecnológicos, sino que también son necesarios los aspectos de gestión, así como los aspectos legales y éticos.

Actualmente, los expertos consideran que la seguridad en los sistemas de información tiene un carácter bidimensional [6]. La seguridad en los sistemas de información ya no se trata como un aspecto exclusivamente técnico, en el que el uso correcto de ciertos mecanismos de seguridad (ej.: protocolos de seguridad, esquemas de cifrado, etc.) garantiza la seguridad de un sistema en términos absolutos. Además, y dada la integración social de los sistemas software, existe una nueva dimensión que cobra gran relevancia y que debe ser analizada detenidamente. Esta nueva dimensión tiene un carácter eminentemente social y organizativo y está ligada a la cada vez mayor interacción de los humanos con los sistemas de información seguros. Resultados de investigaciones han demostrado que el factor humano posee un impacto significativo en la seguridad [7].

El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las PYMES en los países desarrollados suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridad olvidados [8]. Esto puede deberse a que las PYMES carecen de los recursos, tiempo y conocimientos especializados para coordinar la seguridad de la información u ofrecer información adecuada sobre la seguridad, la formación y la educación [8]. Sin embargo, la literatura sugiere una explicación muy diferente. [9] dicen que las PYMES no quieren pagar por la seguridad, y que prefieren mantener una seguridad física con la que están familiarizados. [8] señalan que, al carecer de un conocimiento especializado de tecnologías de seguridad, las PYMES suelen mantener la seguridad con las tecnologías con las que ya están familiarizados. Así mismo, las PYMES no ven la seguridad vinculada a la estrategia empresarial, lo que impacta directamente en el cumplimiento de la misma [10]. De hecho, una investigación reciente pone de

manifiesto la necesidad de vincular la seguridad de la información con los sistemas de información de planificación estratégica y, por tanto, con los objetivos de la empresa [11].

A pesar de que existen numerosos estándares de seguridad en las TIC, como el código de buenas prácticas [12], metodologías para la gestión de la seguridad como COBIT [13], o para el análisis y la gestión de riesgos como Magerit [14], e incluso modelos de madurez para la gestión de la seguridad de los sistemas de información como SSE–CMM [15], éstos suelen estar diseñados para grandes corporaciones, son muy rígidos y su aplicación práctica en pequeñas y medianas empresas requiere de mucho tiempo y suele ser muy costosa. Estos motivos hacen que muchas compañías ofrezcan resistencia a la implantación de técnicas de gestión de seguridad adecuadas, asumiendo de este modo unos riesgos de seguridad, y por tanto de pérdida de competitividad, que resultan inaceptables en la empresa moderna.

En numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las PYMES la utilización de las metodologías y modelos de madurez para la gestión de la seguridad tradicionales, que han sido concebidos para grandes empresas [16-19]. Se justifica en repetidas ocasiones que la aplicación de este tipo de metodologías y modelos de madurez para las PYMES es difícil y costosa.

En el presente articulo describimos la metodología que hemos desarrollado para la gestión de la seguridad en las PYMES, que pretende solucionar los problemas detectados en las metodologías clásicas, las cuales no se están mostrando eficientes a la hora de su implantación en las PYMEs debido a su complejidad y otra serie de factores que serán analizados con detalle en las siguientes secciones del artículo.

El artículo continúa en la Sección 2, describiendo brevemente las metodologías y modelos para la gestión de la seguridad existentes y su tendencia actual. En la Sección 3 se introduce nuestra propuesta de metodología para la gestión de la seguridad orientado hacia las PYMEs. En la Sección 4 se muestra la herramienta desarrollada para dar soporte a la metodología. Finalmente, en la Sección 5 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2 Trabajo relacionado

En los últimos años han aparecido un gran número de procesos, marcos de trabajo y métodos para la gestión de la seguridad de la información, cuya necesidad de implantación está siendo cada vez más reconocida y considerada por las organizaciones, pero que como se ha mostrado, son ineficientes para el caso de las PYMES.

Entre ellas destaca el modelo presentado en la ISO/IEC27001 [20], el de COBIT [13] y el modelo de madurez de la gestión de la seguridad de la información [21]. [22] y [23] investigan la coexistencia y uso complementario de COBIT [13] y la ISO/IEC17799 [24] desarrollando un mapa para la sincronización de ambos marcos de referencia. Algunos de los detractores de la ISO/IEC17799 [24] presentan como desventaja que es una guía de soporte, pero que no alcanza todo el marco necesario para el gobierno de las tecnologías de la información. Su principal ventaja frente a COBIT [13] es que es más detallada y tiene más guías orientadas a cómo deben

hacerse las cosas. Un reciente informe del Instituto para el gobierno de la tecnología de la información (ITGI) soluciona el problema de sincronización desarrollando el mapa entre COBIT [13] y la ISO/IEC17799 [24].

Siguiendo esta "filosofía" también se han propuesto otros muchos modelos de madurez más específicos: para gestión de proyectos [25], ingeniería de requisitos [26], desarrollo distribuido [27], mantenimiento [28], outsourcing [29], arquitecturas [30-33], seguridad [15], servicios e–Government [34], etc.

En numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las PYMES la utilización de las metodologías y modelos de madurez para la gestión de la seguridad tradicionales, que han sido concebidos para grandes empresas [18]. Se justifica en repetidas ocasiones que la aplicación de este tipo de metodologías y modelos de madurez para las PYMES es difícil y costosa. Además, las organizaciones, incluso las grandes, tienden más a adoptar grupos de procesos relacionados como un conjunto que a tratar los procesos de forma independiente [35].

El problema principal de todos los modelos de gestión de la seguridad y su madurez presentados es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que:

- Unos fueron desarrollados pensando en organizaciones grandes (ISO/IEC27001, COBIT) y en las estructuras organizativas asociadas a éstas.
- Otros (ISM3, etc) han intentando centrarse en los problemas de las PYMES, pero son modelos incompletos que sólo afrontan parte del problema, o intentan aportar unas guías básicas de los pasos a realizar, pero sin entrar en cómo gestionar realmente el SGSI. Además, la mayoría son modelos teóricos y están todavía en desarrollo.

3 MGSM-PYME: Metodología para los SGSI en las PYMES

La metodología para la gestión de la seguridad y su madurez en las PYMES que se ha desarrollado, permite a cualquier organización gestionar, evaluar y medir la seguridad de sus sistemas de información, pero está orientado principalmente a las PYMES, ya que son las que tiene mayor tasa de fracaso en la implantación de las metodologías de gestión de la seguridad existentes.

Uno de los objetivos perseguidos en la metodología MGSM–PYME es que sea sencilla de aplicar, y que el modelo desarrollado sobre ella permita obtener el mayor nivel de automatización posible con una información mínima, recogida en un tiempo muy reducido. En la metodología se ha priorizado la rapidez y el ahorro de costes, sacrificando para ello la precisión que ofrecían otras metodologías. Es decir, la metodología desarrollada pretende generar una de las mejores configuraciones de seguridad pero no la óptima, priorizando los tiempos y el ahorro de costes frente a la precisión, aunque garantizando que los resultados obtenidos tengan la calidad suficiente.

Otra de las principales aportaciones que presenta la metodología que se ha desarrollado es un conjunto de matrices que permiten relacionar los diferentes componentes del SGSI (controles, activos, amenazas, vulnerabilidades, criterios de riesgo, procedimientos, registros, plantillas, instrucciones técnicas, reglamentos y

métricas) y que el modelo utilizará, para generar de forma automática gran parte de la información necesaria, reduciendo de forma muy notable los tiempos necesarios para el desarrollo e implantación del SGSI. Este conjunto de interrelaciones entre todos los componentes del SGSI, permite que el cambio de cualquiera de esos objetos altere el valor de medición del resto de objetos de los que se compone el modelo, de forma que se pueda tener en todo momento una valoración actualizada de cómo evoluciona el sistema de seguridad de la compañía.

De esta forma y a partir de la información obtenida mediante la implantación en diferentes empresas, se ha desarrollado una metodología de gestión y madurez de la seguridad de los sistemas de información y un modelo asociado a la misma (ver Fig. 1).

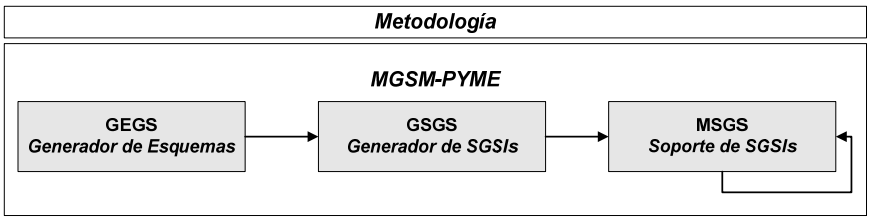

Fig. 1. Subprocesos de la metodología.

Está metodología consta de tres subprocesos principales:

- GEGS – Generación de Esquemas de Gestión de Seguridad.
- GSGS – Generación de Sistemas de Gestión de Seguridad.
- MSGS – Mantenimiento del Sistema de Gestión de Seguridad.

La generación de esquemas es una labor que será realizada por los expertos en seguridad y aunque su elaboración es un proceso costoso, se ve compensado por las enormes reducciones de costes que produce en los otros subprocesos al poder ser reutilizado por compañías con características parecidas (mismo sector y mismo tamaño).

3.1 GEGS – Generación de Esquemas de Gestión de Seguridad.

La Generación de Esquemas para la Gestión de la Seguridad (GEGS), es el primer subproceso de la metodología MGSM–PYME y su objetivo principal es producir un esquema que contenga todas las estructuras necesarias para generar un SGSI y aquellas relaciones que puedan establecerse entre ellas para un determinado tipo de compañías (del mismo sector y tamaño), con el objetivo de ahorrar tiempo y recursos a la hora de generar un SGSI para una compañía que comparta la misma características que aquellas para las que fue creado el esquema. En la Fig. 2 se pueden ver con detalle los diferentes objetos que componen el esquema.

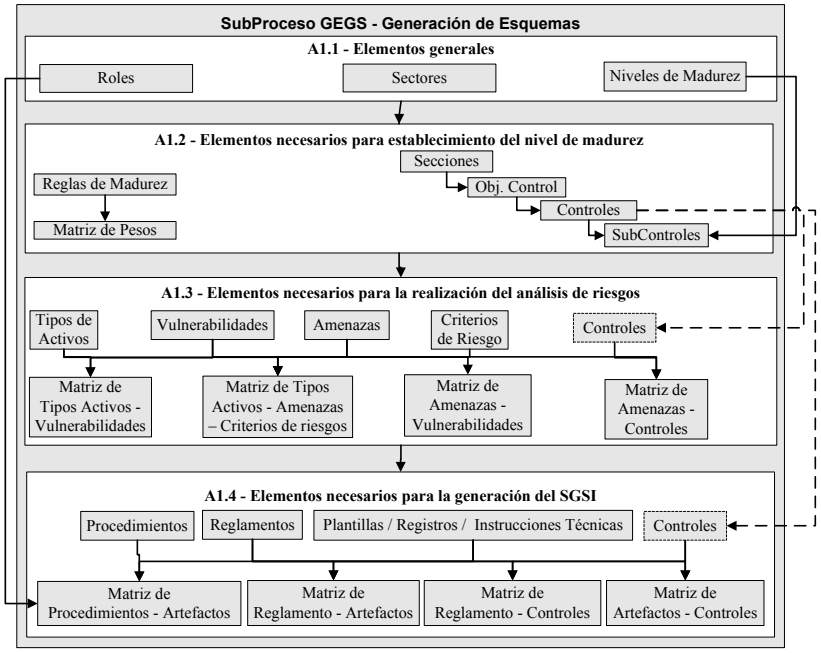

Fig. 2. Elementos del subproceso GEGS.

El subproceso GEGS para la generación de esquemas se compone básicamente de las siguientes actividades:

- A1.1 – Generación de tablas maestras: Se establecen las tablas de configuración iníciales, que contendrán: i) los roles de usuarios del sistema de información que podrán intervenir en el sistema; ii) los diferentes sectores empresariales a los que puede pertenecer la compañía; y iii) los niveles de madurez sobre los que podrá evolucionar el SGSI a lo largo de su ciclo de vida.
- A1.2 – Generación de tablas del nivel de madurez: Se seleccionarán las reglas de madurez que permitirán determinar el nivel de madurez actual del SGSI de la compañía y la lista de controles que se podrán establecer. Los controles se dividirán en subcontroles para poder aproximar el nivel en que estos se cumplen actualmente con mayor precisión. Estos subcontroles tendrán asociados los niveles de madurez definidos en la actividad anterior.
- A1.3 – Generación de tablas del análisis de riesgos: Se selecciona el listado de elementos de los artefactos asociados al análisis de riesgos, así como las relaciones existentes entre ellos.
- A1.4 – Generación de tablas de la biblioteca de artefactos: Se selecciona el listado de elementos de los artefactos asociados a la generación del SGSI, así como las relaciones existentes entre ellos.

Existe una dependencia en la actividad A1.2 ya que requiere una entrada de la actividad A1.1. De igual forma las actividades A1.3 y A1.4 requieren de un elemento de entrada generado durante la actividad A1.2, pero no tienen dependencia entre ellas.

Este subproceso recibirá como entradas:

- Conocimiento de los expertos adquirido durante otras implantaciones de SGSIs. (ej.: relaciones entre elementos, procedimientos, etc).
- Listados de elementos procedentes de otras normas, guias de buenas prácticas (ej.: ISO/IEC27002) o metodologías (ej.: Magerit v2).

Y generará como salida un esquema, que será utilizado por los siguientes subprocesos y que se componen básicamente de los siguientes elementos:

- Un subconjunto de elementos seleccionados de las listas de entrada.
- Una serie de matrices que relacionan entre sí los principales elementos (controles, tipos de activos, vulnerabilidades, amenazas y criterios de riesgo) necesarios para la elaboración de un análisis de riesgos.
- Una serie de matrices que relacionan entre sí los principales elementos (controles, procedimientos, reglamentos, plantillas, registros, instrucciones técnicas) necesarios para la generación del SGSI.

Todo este conjunto de artefactos, necesario para poder generar el sistema de gestión del sistema de información de la compañía, son incluidos en el repositorio de esquemas para el SGSI que se actualiza constantemente con el nuevo conocimiento obtenido en cada nueva implantación.

Debido a la complejidad del desarrollo de un esquema y como parte de la investigación se ha desarrollado un esquema inicial, denominado esquema base (EB), obtenido a partir del conocimiento adquirido durante el proceso de investigación, con el objetivo de posibilitar la creación de nuevos esquemas mediante un proceso de clonación (generar un nuevo esquema a partir de un esquema existente) del esquema base y realizando posteriormente los ajustes necesarios en el nuevo esquema para adecuarlo al tipo de compañías deseada.

3.2 GSGS – Generación del Sistema de Gestión de Seguridad

La Generación del Sistema de Gestión de Seguridad (GSGS), es el segundo subproceso y tiene como principal objetivo la generación del SGSI mediante la selección del esquema más adecuado para el tipo de compañía y la solicitud de información empresarial y técnica a la empresa por medio de un interlocutor (Int), designado por la misma. En la Fig. 3 se pueden ver los diferentes objetos que componen este subproceso.

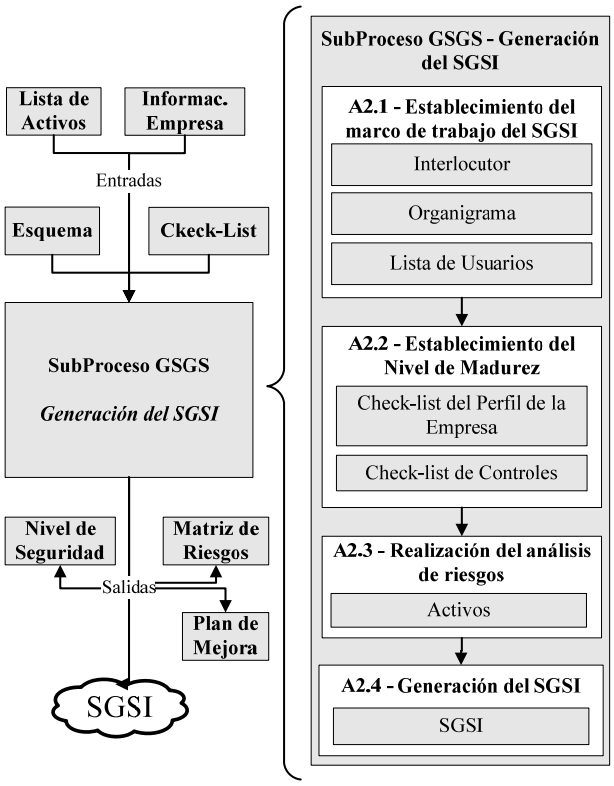

Fig. 3. Elementos del subproceso GSGS.

El subproceso GSGS para la generación del SGSI se compone básicamente de las siguientes actividades:

- A2.1 – Establecimiento del marco de trabajo del SGSI: Se establecerán las relaciones con la compañía, definiendo el interlocutor válido y solicitando información de la misma: i) organigrama de la compañía; ii) usuarios con acceso al sistema de información y roles que desempeñan.
- A2.2 – Establecimiento del nivel de madurez:
    - Se solicita mediante una entrevista de carácter empresarial, información relacionada con la compañía (número de empleados, facturación, etc) con el objetivo de determinar el esquema que más se adecua a ese tipo de compañía de los existentes en el repositorio de esquemas.
    - Se realizará una segunda entrevista de carácter técnico, para determinar con detalle la situación actual de la compañía con respecto a la gestión de la seguridad de su sistema de información.

- A2.3 – Realización del análisis de riesgos: Se identificarán un conjunto de activos básicos de grano grueso, determinando el coste (cualitativo y cuantitativo) que tendría para la organización su pérdida. A partir del conjunto de activos se determinarán los riesgos de seguridad a que están sometidos y se generara un plan para mitigar los riesgos de seguridad de una forma eficiente.
- A2.4 – Generación del SGSI: A partir de toda la información obtenida y del esquema seleccionado, se generan los elementos que conformarán el SGSI para la compañía y se procederá a la implantación del mismo en la compañía.

Este subproceso recibirá las siguientes entradas:

- Información de la compañía sobre la que se desea realizar el SGSI: i) información empresarial; ii) interlocutor válido para el desarrollo del SGSI; iii) organigrama de la compañía; iv) el listado de usuarios y los roles que desempeñan dentro del sistema de información de la compañía.
- El esquema más adecuado para generar el SGSI a partir del perfil empresarial de la compañía y del repositorio de esquemas.
- Dos listas de verificación: i) una lista de verificación con información del negocio; ii) una lista de verificación con información sobre el nivel de la gestión de la seguridad.
- Un listado de los activos asociados al sistema de información de la compañía, intentando agruparlos en el menor número de activos posibles (grano grueso), para reducir el coste de generación y gestión del sistema de información.

Y generará las siguientes salidas, que contienen una descripción completa del SGSI de la compañía:

- El nivel de madurez actual de la compañía con respecto a su sistema de gestión de seguridad de la información y hasta qué nivel de madurez debería progresar.
- Una matriz con los riesgos a los que están sometidos los activos de la compañía.
- Un plan de mejora ordenado, que indica qué controles deben ser reforzados para que el nivel de seguridad de la compañía evolucione lo más rápido posible.
- Un conjunto de elementos que componen el SGSI de la compañía, que incluyen: i) un cuadro de mandos que indicara el nivel de seguridad para cada control relacionado con la gestión de la seguridad; ii) un conjunto de reglamentos, plantillas e instrucciones técnicas válidos para esa compañía en el momento actual; iii) un conjunto de métricas; iv) un conjunto de usuarios, asociados a roles que permitirán ejecutar una serie de procedimientos para interactuar con el sistema de información; v) y un conjunto de reglamentos que se deben cumplir para el funcionamiento del SGSI.

Todo este conjunto de objetos, que componen el SGSI, son incluidos en el repositorio de SGSIs y serán utilizados por la compañía para poder gestionar correctamente la seguridad del sistema de información.

3.3 MSGS – Mantenimiento del Sistema de Gestión de Seguridad.

El Mantenimiento del Sistema de Gestión de Seguridad (MSGS) es el tercer subproceso definido en MGSM–PYME y su principal propósito es permitir realizar el conjunto de tareas necesarias para poder trabajar con el SGSI, poder medir la evolución del mismo y facilitar la obtención de conocimiento para la mejora continua de los esquemas y los SGSI generados. En la Fig. 4 se pueden ver los diferentes objetos que componen este subproceso.

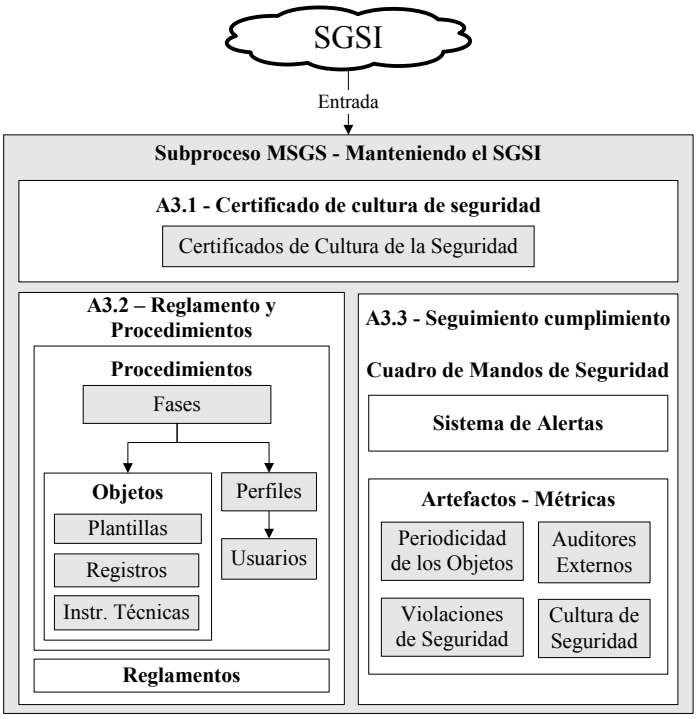

Fig. 4. Elementos del subproceso MSGS.

El subproceso MSGS para el mantenimiento del SGSI se compone básicamente de las siguientes actividades:

- A3.1 – Obtener o renovar el certificado de cultura de seguridad: Se establecerá un sistema que permita crear de forma progresiva una conciencia de seguridad entre los usuarios del sistema de información, que garantice la calidad del mismo.
- A3.2 – Ejecutar procedimientos del SGSI: Se ejecutarán procedimientos generales y específicos (ej.: procedimiento de denuncia) que permitirán mantener actualizado el SGSI de la compañía.

- A3.3 – Seguimiento del cumplimiento del SGSI: Se dispondrá de un conjunto de métricas para mantener actualizado de forma dinámica y en tiempo real el cuadro de mandos de seguridad de la compañía, de forma que el responsable de seguridad podrá tomar decisiones sin necesidad de esperar a la realización de una auditoría externa.

Este subproceso recibirá las siguientes entradas, procedentes del subproceso anterior:

- Un conjunto de usuarios y los roles que desempeñarán dentro del sistema de información, que determinarán a qué procedimientos tienen acceso.
- Un conjunto de reglamentos que se deben cumplir para el buen funcionamiento del SGSI.
- Un conjunto de procedimientos de seguridad, y los elementos (plantillas, registros, instrucciones técnicas) asociados a los mismos.
- Un cuadro de mandos que indicara el nivel de seguridad para cada control relacionado con la gestión de seguridad de la compañía.

Y generará las siguientes salidas:

- Una serie de instancias de los procedimientos existentes, que se irán ejecutando a lo largo del tiempo y que permitirán gestionar y mantener el SGSI de la compañía.
- Un conjunto de métricas que permitirán mantener actualizado el cuadro de mandos asociado al nivel de seguridad del sistema de gestión de seguridad de la información: i) un conjunto de métricas generales; ii) métricas especificas: periodicidad de los objetos, violaciones de seguridad, conciencia de seguridad y auditoras externas.
- Estadísticas extraídas del uso diario del SGSI por los usuarios del sistema de información, que se convertirá en conocimiento para que los expertos en seguridad puedan elaborar nuevos esquemas y refinar los existentes.

Toda la información de salida generada durante la vida útil del SGSI, será incluida en el repositorio de información del SGSI y será utilizada por la compañía para poder gestionar correctamente la seguridad del sistema de información y por el grupo de expertos de seguridad para mejorar los esquemas del subproceso GEGS.

4 MGSM-TOOL: Automatización de la metodología.

Para validar la metodología MGSM-PYME, se ha desarrollado una herramienta denominada MGSM-TOOL que permite desarrollar modelos de gestión de seguridad sencillos, económicos, rápidos, automatizados, progresivos y sostenibles, que son los principales requerimientos que tienen este tipo de compañías a la hora de implantar estos modelos.

Desde el punto de vista de usuario la herramienta presenta dos ventajas claras:

- Simplicidad: Todas las actividades del SGSI se han orientado a reducir la complejidad del proceso de construcción y mantenimiento de un SGSI, pensando en organizaciones (PYMES) cuyas estructuras organizativas son muy sencillas.
- Automatización: Todo el sistema utiliza un concepto denominado esquemas para poder automatizar los pasos necesarios para construir y mantener el SGSI de la compañía.

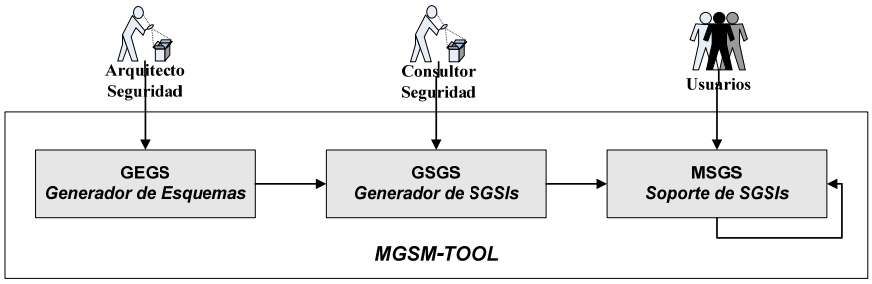

Fig. 5. Zonas de la aplicación MGSM-TOOL.

La herramienta se compone de tres partes claramente diferenciadas que se pueden ver en la Fig. 5, y que se corresponden con los subprocesos de la metodología:

- Generador de Esquemas (GEGS): Esta zona de la herramienta es sólo accesible por el arquitecto de gestión de la seguridad (AGS) y el grupo de expertos del dominio (GED), y desde ella pueden realizar tres operaciones básicas: i) Crear nuevos esquemas; ii) Clonar esquemas a partir de un esquema existente; y iii) Modificar esquemas para mejorar la generación del SGSI.
- Generador del SGSI (GSGS): Esta zona de la herramienta es sólo accesible por el consultor de seguridad (CoS) y su objetivo es generar el SGSI para la compañía.
- Soporte del SGSI (MSGS): Esta zona de la herramienta es accesible por los usuarios del sistema de información. El perfil que más relevancia tiene dentro de esta zona es el responsable de seguridad (RS). Desde ella se pueden realizar tres operaciones básicas: i) Gestión de los certificados de cultura de la seguridad; ii) Gestión de procedimientos; y iii) Gestión del cuadro de mandos.

Los esquemas son el núcleo sobre el que se desarrolla la herramienta, ya que permiten la automatización de los SGSIs. Estos esquemas están formados por un conjunto de elementos y asociaciones entre ellos, definidos a partir del conocimiento adquirido por los clientes.

La herramienta ha permitido reducir los costes de implantación de los sistemas y supone un mayor porcentaje de éxito de las implantaciones en las PYMES. Por estas razones, se considera que los resultados de esta investigación pueden ser muy positivos para las PYMES, ya que les permite acceder al uso de sistemas de gestión de la seguridad con un coste de recursos razonable para su tamaño. Además, mediante

el uso de la metodología y la herramienta que la soporte, se pueden obtener resultados a corto plazo y reducir los costes que supone el uso de otros modelos y herramientas, consiguiendo un mayor grado de satisfacción y eficiencia en la empresa.

Adicionalmente, la herramienta permite mantener repositorios con información acerca de las especificaciones de los esquemas necesarios para construir los SGSI y con información de los resultados obtenidos en los diferentes casos de uso, lo que permite mejorar constantemente la metodología y los modelos.

5 Conclusiones y futuros trabajos.

En este artículo se ha presentado la propuesta de una nueva metodología para la gestión de la seguridad y su madurez en las PYMES. Esta metodología permite a las PYMES desarrollar y mantener un SGSI con un coste en recursos aceptable para este tipo de compañías.

Para demostrar la validez de la metodología se ha definido un modelo (esquema base) que permite soportar los resultados generados durante la investigación y que cumple con los objetivos perseguidos.

Se ha definido cómo se debe utilizar esta metodología y las mejoras que ofrece con respecto a otras metodologías que afrontan el problema de forma parcial, o de manera demasiado costosa para las PYMES.

Las características ofrecidas por la nueva metodología y su orientación a las PYMES ha sido muy bien recibida, y su aplicación está resultando muy positiva ya que permite acceder a este tipo de empresas al uso de sistemas de gestión de seguridad de la información, algo que hasta ahora había estado reservado a grandes compañías. Además, con esta metodología se obtienen resultados a corto plazo y se reducen los costes que supone el uso de otras metodologías, consiguiendo un mayor grado de satisfacción de la empresa.

Finalmente, se considera que el trabajo realizado debe ser ampliado con nuevas especificaciones, nuevos esquemas, ampliando el conjunto de artefactos de la biblioteca y profundizando en el modelo con nuevos casos de ejemplo.

Entre las mejoras del modelo sobre las que se esta trabajando de cara al futuro destacan:

- Mejoras asociadas al subproceso GEGS: Adaptación de los esquemas predefinidos para PYMES con las nuevas normas y estándares que surjan asociados a la gestión de la seguridad.
- Mejoras asociadas al subproceso GSGS: Revisar aspectos relacionados con la generación del SGSI.
- Mejoras asociadas al subproceso MSGS: Mejorar y aumentar los mecanismos de medición y auto–evaluación de la seguridad introduciendo nuevas métricas en el modelo que permitan conocer en todo momento el nivel de la seguridad, minimizando el número de auditorías de auto–ajuste necesarias para mantener actualizado dicho nivel de seguridad.

Todas las mejoras futuras de la metodología y el modelo se están orientando a mejorar la precisión del mismo, pero siempre respetando el principio de coste de

recursos, es decir, se busca mejorar el modelo sin incurrir en costes de generación y mantenimiento del SGSI.

Mediante el método de investigación "investigación en acción", con la ayuda de la retroalimentación obtenida directamente de nuestros clientes, esperamos conseguir una mejora continua de estas implantaciones.

Agradecimientos

Esta investigación es parte de los proyectos ESFINGE (TIN2006-15175-C05-05), concedido por el Ministerio de Educación y Ciencia y QUASIMODO (PAC08-0157-0668) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha.

Referencias

1. Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. 43(7): p. 125-128.
2. Masacci, F., M. Prest, and N. Zannone, *Using a security requirements engineering methodology in practice: The compilanse with the Italian data protection legislation.* Computer Standards & Interfaces, 2005. 27: p. 445-455.
3. Walker, E., *Software Development Security: A Risk Management Perspective.* The DoD Software Tech. Secure Software Engineering, 2005. 8(2): p. 15-18.
4. Humphrey, E. *Information security management standards: Compliance, governance and risk management.* in *Information Security Tech. Report*. 2008.
5. Tsujii, S. *Paradigm of Information Security as Interdisciplinary Comprehensive Science*. in *International Conference on Cyberworlds (CW'04)*. 2004: IEEE Computer Society.
6. Siponen, M.T., *Information Security Standards Focus on the Existence of Process, Not Its Content?*, C.o.t. ACM, Editor. 2006. p. 97-100.
7. Schumacher, M., *Security Engineering with Patterns*. Lecture Notes in Computer Science. Vol. 2754. 2003: Springer-Verlag. 208.
8. Gupta, A. and R. Hammond, *Information systems security issues and decisions for small businesses.* Information Management & Computer Security, 2005. 13(4): p. 297-310.
9. Johnson, D.W. and H. Koch. *Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive?* in *39th Annual Hawaii International Conference on System Sciences (HICSS'06)*. 2006.
10. O'Halloran, J., *ICT business management for SMEs.* Computer Weekly, 2003. December 11.
11. Doherty, N.F. and H. Fulford, *Aligning the Information Security Policy with the Strategic Information Systems Plan.* Computers & Security, 2006. 25(2): p. 55-63.
12. ISO/IEC17799, *ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management*. 2005.
13. COBITv4.0, *Cobit Guidelines, Information Security Audit and Control Association*. 2006.
14. MageritV2, *Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2*. 2005, Ministerio de Administraciones Públicas.
15. SSE-CMM, *Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.* 2003.

16. Batista, J. and A. Figueiredo, *SPI in very small team: a case with CMM.* Software Process Improvement and Practice, 2000. 5(4): p. 243-250.
17. Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. 6: p. 67-83.
18. Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. 9: p. 23-31.
19. Calvo-Manzano, J.A., *Método de Mejora del Proceso de desarrollo de sistemas de información en la pequeña y mediana empresa (Tesis Doctoral). Universidad de Vigo*. 2000.
20. ISO/IEC27001, *ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements.* 2005.
21. ISM3, *Information security management matury model (ISM3 v.2.0)*. 2007, ISM3 Consortium.
22. Von Solms, B., *Information Security governance: COBIT or ISO 17799 or both?* Computers & Security . 2005. 24: p. 99-104.
23. Pertier, T.R., *Preparing for ISO 17799.* Security Management Practices, 2003. jan/feb: p. 21-28.
24. ISO/IEC17799, *ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management*. 2005.
25. McBride, T., B. Henderson-Sellers, and D. Zowghi. *Project Management Capability Levels: An Empirical Study.* in *11th Asia-Pacific Software Engineering Conference (APSEC'04)*. 2004: IEEE Computer Society.
26. Sommerville, I. and J. Ransom, *An Empirical Study of Industrial Requirements Engineering Process Assessment and Improvement.* ACM Transactions on Software Engieering and Methodology, 2005. 14(1): p. 85-117.
27. Ramasubbu, N., M.S. Krihsnan, and P. Kompalli, *Leveraging Global Resources: A Process Maturity Framework for Managing Distributed Development.* IEEE Software, 2005: p. 80-86.
28. April, A., et al., *Software Maintenance Maturity Model: the software maintenance process model. Journal of Software Maintenance and Evolution.* Research and Practice, 2005. 17: p. 197-223.
29. KcKinney, C., *Capability Maturity Model and Outsourcing: A Case for Sourcing Risk Management.* Information Systems Control, 2005. 5.
30. OMB, *OMB Enterprise Architecture Assessment v 1.0. The Office of Management and Budget, The Executive Office of the President.* 2004.
31. Van der Raadt, B., J.F. Hoorn, and H. Van Vliet. *Alignment and Maturity are siblings in architecture assesment*. in *Caise 2005*. 2005.
32. NASCIO, *National Association of State Chief Financial Officers. Enterprise Architecture Maturity Model, Version 1.3. National Association of State Chief Financial Officers*. 2003: Lexington KY.
33. Schekkerman, J., *Extended Enterprise Architecture Maturity Model. Institute for Enterprise Architecture Developments (IFEAD)*. 2003: Amersfoort, The Netherlands.
34. Widdows, C. and F. Duijnhouwer, *Open Source Maturity Model. Cap Gemini Ernst & Young*. 2003: New York NY.
35. Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. 7(3): p. 4-13.